# فيروسات الحاسب وكيفية تصنعها

المحتويات:-

مقدمة:-
بسم الله الرحمن الرحيم
تعتبر الفيروس خطر شديد من اشد الاخطار التي تواجه عصر الحاسب الالي الان ، حيث يعد الانتشار الرهيب والمتزايد في اعداد الفيروسات خطر علي امن المعلوماتية في العالم، ونظرا للانتشار الرهيب للفيروسات ومع الجهل الشديد من الكثير من المستخدمين بماهية الفيروسات فإن العديد من مستخدمي الحاسب الالي لديهم لبس في بعض المفاهيم التي تتعلق بالفيروسات والحماية علي الانترنت وغيرها ، فكثير من المستخدمين يخلط بين الانواع المختلفة من البرامج الخبيثة والبعض الاخر من المستخدمين لايعلم اي شئ عن هذة البرامج الخبيثة المنتشرة في اجهزة الكمبيوتر علي مستوي العالم ، ونظرا لانتشار الكثير من المعلومات الخاطئة فيما يتعلق بالفيروسات والقرصنة والحماية علي شبكة الانترنت كان لابد من البحث والتدقيق في المعلومات الموجودة علي الانترنت من اجل تقديم المعلومة الصحيحة للمستخدم من اجل ان تتضح للمستخدم الصورة الحقيقية للواقع المسمي بالفيروسات حتي لايتعرض المستخدمين لهذا الخطر الموجود في اغلب الاماكن علي شبكة الانترنت، ومن هذا المنطلق عزيزي القارئ قمت بالبحث وجمع المعلومات الصحيحة من مصادر موثوقة علي الشبكة العنكوبتية ومن الكتب والمراجع فيما يتعلق بالفيروسات والحماية علي امل ان اوصل المعلومة الصحيحة للمستخدم من اجل ان اوضح للمستخدم المعلومات الغامضة عن الفيروسات والتي يعتبرها المستخدم الوحش المدمر الذي هدفة الوحيد هو نفس وتدمير البيانات الموجوده علي الحاسب ، وسنعرف فيما بعد ان اغلب مانعرفة من معلومات عن الفيروسات هي مجرد تهويل علي المستخدم من اجل الاحساس بالخطر المحدق بة من هذة البرامج الخبيثة.
في هذة السلسلة بإذن الله تعالي سوف نتحدث عن الفيروسات وانواعها وكيفية برمجتها والادوات اللازمة لبرمجتها وسنعرض الامثلة لاغلب الفيروسات الشهيرة وسنقوم بتحليلها من الصفر من اجل الوقوف علي حقيقة هذة البرامج من اجل توضيحها للمستخدم حتي يكون علي دراية بما تحدثة هذة البرامج في حاسبة الشخصي.

ماهو الفيروس:-
لقد ظهرت العديد من التعريفات للفيروسات منذ بداية ظهورها في عالم الكمبيوتر ولكن قد قمت بجمع هذة التعريفات في تعريف واحد مفصل موضحات ماهو فيروس الحاسب الالي، فاستطيع القول بأن:-
فيروسات الحاسب هي برامج مستقلة بذاتها صممت عمدا من قبل مبرمجين محترفين بهدف تحقيق اهداف معينة من وراء برمجتها وهذة البرامج تتميز بقدرة شديدة علي الانتشار والتوسع في شبكات الحاسب الالي نظرا لبرمجتها علي كيفية التناسخ من جهاز الي اخر عن طريق وسائل الاتصال المتاحة ، ومن هذا التعريف الطويل يمكنن توضيح النقاط التالية ، اولا الفيروسات برامج عادية شأنها شأن برامج الحاسب الاخري الا انها تتميز عن باقي البرامج بعدة ميزات انها قادرة علي ان تنسخ نفسها داخل النظام او بمعني تمت برمجتها لكي تقوم بنسخ نفسها داخل النظام من اجل السيطرة علي النظام لاي هدف كان، ثانيا تعتبر الفيروسات برامج مستقلة بذاتها اي انها لاتحتاج الي اي ملفات مساعده اخري لكي تعمل فمثلا لايشترط لكي يعمل فيروس ان يتوفر لديك برنامج معين بل ان الفيروس مستقل لايحتاج الي اي ملفات معة كل مايحتاجة مدموج بداخلة وسنتعرف فيما بعد علي كيفية دمج كل مايحتاجة الفيروس من ادوات وبرامج معة لكي يقوم بوظيفتة المسندة الية علي اكمل وجة، ثالثا الفيروسات لاتكون ضارة الا في حالة عملها بمعني ان الفيروس لايسبب لك اي ضرر الا اذا قمت بتشغيلة وهذة نقطة مهمة اذ ان الكثير من المستخدمين يظن انة بمجرد دخول برنامج بة فيروس الي حاسبك فقد هلك النظام اقول لك عزيزي المستخدم ان الفيروس لن ينشط من تلقاء نفسة بل يحتاج الي ان يقوم برنامج او تقوم انت بتشغيلة ومن ثم لن تستطيع السيطرة علية وهذة نقطة مهمة لانة لابد للمستخدم من ان يقوم بتشغيل الفيروس حتي يعمل لانة لن يعمل من تلقاء نفسة ، رابعا وهذة نقطة اخري مهمة في الفيروسات وهي ان الفيروسات يجب ان تحتوي علي ميكانيكية خاصة بنسخ الفيروس وانتشاره لان البرنامج الخبيث لكي يحمل لقب فيروس لابد وان يقوم بنسخ نفسة اكررها يجب ان يقوم بنسخ نفسة الي النظام لانة بدون نسخ الفيروس نفسة الي النظام لن يتمكن من الانتشار وبالتالي لن يمثل تهديد وبالتالي لن يطلق علية فيروس لانة انتهي في مكانة.

ومن هذا التعريف يتضح لك عزيزي القارئ ان الفيروسات ليس هدفها الاول هو تدمير بياناتك او نسف ملفاتك بل الهدف الاول هو الانتشار ومن ثم تحقيق الهدف المطلوب منها.
ومن المثير ايضا انني وجدت في اغلب المواقع اشخاص يروجون لاكواد وبرامج لايعلمون ماهي وكيفية عملها ويطلقون عليها اكواد للفيروسات وبرامج لتصنيع الفيروسات انا اقول لك عزيزي الكاتب تعلم اولا واعرف ماهي الفيروسات ثم تحدث كما يحلوا لك  لكن لاتقم بنشر اي معلومات علي سبيل جلب الزوار ومن ثم تنشر معلومات خاطئة ، ففي احد  المواقع وجد احد الكتاب يضع شفرة تقوم بعمل فورمات للقرص الصلب :C قل لي عزيزي القاري كيف سيتمكن النظام من عمل الفورمات اذا كان هذا القرص هو المحتوي علي نظام التشغيل ، هذا ان دل فإنما يدل علي جهل الكاتب بالحاسب الالي كليا فهو لايدري اي معلومات حتي عن نظام التشغيل ، وهناك من هذة المواقع الكثير اما هنا عزيزي القارئ فإنني سوف اضع المعلومة بين يديك بعد ان اجري عليها العديد من الاختبارات حتي اتاكد لك من صدق المعلومة حتي لاتقع عزيزي القارئ فريسة للمعلومات الخاطئة.

أنواع البرامج الخبيثة:-
يوجد هناك العديد من انواع البرامج الخبيثة في عالم الكمبيوتر والتي تعتبر الفيروسات نواعا من هذة الانواع اما باقي الانواع فهي برمجيات اخري لها خصائص اخري واهداف اخري تختلف عن الفيروسات ولكنهم جميعا يشتركون في شئ واحد وهو انها برامج خبيثة هدفها هدف غير شرعي.
اما بالنسبة للانواع فلن اذكرها كلها بل ساكتفي بذكر الانواع التي قد نحتاجها نحن في هذة المجموعه اما باقي الانواع فسنقوم بشرحها بالتفصيل في موضوعات اخري ان شاء الله تعالي.
الانواع:-

١. Viruses
٢. Downloaders
٣. Adwares
٤. Worms
٥. Droppers
٦. Trojan Horses
٧. Hack Tools
٨. Patches, Cracks , KeyGen and trainers

وكما قلت فان هذة الانواع هي الانواع الاساسية وهناك الكثير من الانواع ولكن سنتحدث عنها بالتفصيل في مواضيع اخري ان شاء الله تعالي.
سنبدا الان بتوضيع هذة الانواع واحدا واحدا بالتفصيل:-

**<u>Viruses</u>**

الفيروسات وهي محور حديثنا وكما قمنا بتعريفها من قبل علي انها برامج قادرة علي الانتشار والتناسخ بشكل رهيب في النظام بدون علم المستخدم وكما قلنا ايضا انها برامج مستقلة بذاتها اي لاتحتاح الي اي اضافات او برامج خاصة لكي تعمل فهي تعمل علي النظام المصممة لة بدون اي مشاكل، وهي برامج متخصصة اي ان لها هدف من برمجتها وإلا فلن تعمل بالشكل المطلوب منها.

**<u>Downloaders</u>**

سنقوم بترجمة هذة الكلمة علي انها "برامج تحميل" اي هذا النوع من البرامج الخبيثة لايتميز بقدرة علي الانتشار بل ان كل

مايقوم بعملة هو ان يقوم بتحميل برنامج من علي الانترنت الي جهاز الضحية ومن ثم يقوم هذا البرنامج نتشغيلة فمثلا انت تقوم بتحميل ملف من الانترنت وهذا الملف يحتوي علي داونلودر سيقوم هذا الداونلودر بتحميل ملف اخر من الانترنت وهو عباره عن الفيروس او البرنامج الاخر وبعد اكتمال تحميلة يقوم بتشغيلة وبهذا تنتهي وظيفتة ومع العلم كل هذا يتم بدون علم المستخدم.

وتتميز الداونلودرز بالخصائص التالية:-

١. برامج صغيرة الحجم.
٢. لها ايقونة مخادعه. كبرنامج مشهور مثلا.
٣. ليس لها اي نافذة عند التشغيل.
٤. من الممكن ان يكون لها رساله خطأ مخادعه.
٥. تحذف نفسها بعد اكتمال مهمتها.
٦. تنسخ نفسها في مكان امن في النظام لحين انتهاء مهمتة.

من الممكن ان ياتي اليك الدونلودر كمرفق في رسالة لذلك يجب فحص المرفقات ببرنامج الحماية ، والدونلودرز لاتشغل حيز من ذاكرة الحاسب لذلك فان الاحساس بها في النظام يعد امر صعب علي المستخدم العادي وحتي علي بعض المحترفين، وتتميز هذة البرامج بصغر حجمها لدرجة ان حجمها لايتجاوز ٣٠ ك ب.

**Adwares(Advertisements Software)**

كما يترجمها الكثير بـ برامج الاعلانات ، هذا النوع من البرامج الخبيثة لايمثل تهديدا علي الحاسب بل يمثل التهديد الاكبر علي مستخدم الحاسب لان الهدف من تصميم هذة البرامج هو ليس الإضرار بملفات او ببيانات المستخدم بل الهدف منها هو عرض الاعلانات بالقوة علي المستخدم او اجبار المستخدم علي زيارة مواقع وغالبا مايستخدم هذا النوع من البرامج في الترويج للمواقع الاباحية وغيرها من المواقع التي تتبع سياسة العمل القذر.

تتميز هذة البرامج بالاتي:-

١. صغيرة الحجم.
٢. لها ايقونة مثيرة كي تجبرك علي فتحها.
٣. لها هدف دعائي.
٤. قد تكون برنامج او سكربت في صفحة انترنت.
٥. ليس لها اي نافذة.

## Worms

الديدان وهي من اخطر انواع الفيروسات حيث انها تبرمج بطريقة تجعل ايقاف انتشارها امرا يبدو مستحيلا فكل الهدف من هذة البرامج هو الانتشار ثم الانتشار ثم الانتشار ، فتتمتع هذة البرامج بالقدرة علي نسخ نفسها في وحدات التخزين الخارجية كالفلاشات وكروت الميموري وايضا لها القدرة علي البحث في الشبكة المحلية وإصابة الاجهزة المتصلة عن طريق البحث عن الثغرات في نظام التشغيل ومن ثم استغلالها في الانتشار كما ان لها القدرة علي ارسال نسخها منها كمرفق في البريد الالكتروني الي قوائم البريد المخزنة علي اجهزة الضحايا ، إنها حقا كابوس مرعب يهدد عالم الحاسب الالي، كما ان هذةالبرامج تملك ميكانيكيات تمكنها من دمع نسخ منها في البرامج التنفيذية من نفس النوع حتي تسهل عملية الانتشار وتزيد من سرعتها مدمرة بذلك الملف التنفيذي.

تتميز الديدان بالخصائص التالية:-

١. ايقونة مخادعه. ايقونة مجلد مثلا.
٢. حجم من ١٠٠ ك ب الي ١ م ب.
٣. ليس لها نافذة.
٤. تدمير درع الحماية والجدار الناري.
٥. اصابة جميع الملفات التنفيذية.

## Dropper

لاعرف لها ترجمية دقيقة ولكن يمكننا القول بان الدروبرز برامج خبيثة تقوم بعمل ساعي البريد فهي تقوم بتوصيل برنامج خبيث الي هدفة ومن ثم تنتهي مهمتها قمثلا برنامج يقوم بحمل فيروس الي جهاز اخر ومن ثم بعد توصيل هذا الفيروس يحذف البرنامج نفسة وتنهي مهمتة.

## Trojan Horses

يعتبر هذا النوع من اشهر انواع البرامج الخبيثة الموجودة في مجال الحاسب الالي حيث يستخدم هذا النوع من البرامج الخبيثة في عمليات الاختراق والقرصنة، فهذا النوع من البرامج تتم برمجتة بان يقوم بعد تشغيلة في جهاز الضحية بفتح منفذ في جهاز الحاسب يسمح هذا المنفذ بإجراء الاتصالات مع الحاسب الالي من خلال شبكة الانترنت مما يعرض الحاسب الالي للاختراق بواسطة القراصنة ، ثم بعد ان يقوم بفتح منفذ

في جهاز الكمبيوتر يقوم بإنتظار اي اتصالات قادمة من هذا المنفذ ومن ثم السماح لها بان تتم وتكون هذة الاتصالات من موجه الاوامر الخاص بهذا التروجان اي المخترق ثم بعد ذلك يبدا في استلام الاوامر ومن ثم تنفيذها علي جاز الضحية وتنتهي مهمة التروجان بانتهاء عملية القرصنة ، وبدون الانترنت يصبح هذا النوع من برامج التجسس بلا جدوي لانة لايكوت لة نشاط خطير إلا في حالة وجود الاتصال من قبل المخترق من خلال الانترنت.

وتتميز برامج التجسس او احصنة طروادة بهذة الخصائص:-

١. ذات ايقونة مخادعه كبرنامج شهير مثلا.
٢. اغلبها يتم استقبالها من الانترنت.
٣. حجمها من ١٠ ك ب  الي ٣ م ب .
٤. ليس لها نافذة.
٥. تحتاج الي اتصال بالانترنت لكي تعمل بشكل صحيح.

أساسيات الفيروسات:-

تكلمنا في الموضوعات السابقة من هذه السلسلة عن تعريف الفيروسات وقمنا ايضا بالتعرف علي اشهر انواع هذه الفيروسات ،وسنتحدث هنا بإذن الله تعالي عن اساسيات الفيروسات فليس اي برنامج يقوم بحذف الملفات يجب ان يحمل لقب فيروس فهناك مجموعه من المعايير والشروط التي يجب توافرها في البرنامج الذي تقوم ببرمجتة من اجل الحصول علي لقب فيروس او برنامج خبيث، وسنقوم بتوضيح بنية الفيروس او المنهج الذي تسلكة الفيروسات في عملها.

فيروس الكمبيوتر عادة ما يتكون من ثلاث اجزاء اساسية:-

١. الية التناسخ والانتشار.
٢. المفجر.
٣. المدمر.

وسوف نتحدث بالتفصيل عن كل جزء من اجزاء الفيروس، فبدون اي جزء من هذة الاجزاء الثلاثة لانعتبر ان هذا البرنامج مهما كان الخطر الذي يحتوية هذا البرنامج فيروسا اطلاقا مالم يحتوي علي الثلاثة اجزاء السابقة.

الجزء الاول:الية التناسخ والانتشار:-
تعتبر الية التناسخ والانتشار اهم عنصر في الفيروس وخاصة الفيروسات التي تصمم لكي تصيب اكبر عدد ممكن من الاجهزة فهي المسؤلة عن نسخ الفيروس الي الانظمة المستهدفة وكذلك عمل نسخ من الفيروس في جهاز الحاسب وهي المسؤلة ايضا عن اصابة الملفات التنفيذية بالفيروس وتقوم ايضا بارسال الفيروس عبر الانترنت الي قائمة العناوين البريدية وكذلك هي المسؤلة عن البحث في الشبكة المحلية ان توفرت عن الاجهزة الاخري ومحاولة نشر الفيروس بها، ومما سبق يتضح ان الية التناسخ هي بمثابة برنامج عمل النسخ من الفيروس الي اي مكان ، ومن دون هذة الآلية لن يصبح الفيروس ذا جدوي بل سيظل خاملا في مكانة لايمثل خطرا علي الاجهزة المحيطة ، وتحتوي هذه الالية علي الاوامر الشهيرة مثل الامر نسخ والامر نقل وكذلك الاوامر الخاصة بارسال البريد الالكتروني وسوف نتعرف في الموضوعات القادمة عن كيفية برمجة الية تناسخ

وانتشار بشكل محترف حتي نستطيع اصابة اكبر عدد ممكن من اجهزة الكمبيوتر.

الجزء الثاني: المفجر:-
يعمل المفجر في الفيروس كما يعمل المؤقت في القنبلة ، فكلنا شاهدنا في الافلام المختلفة كيف تعمل القنبلة حيث تحتوي علي مؤقت صغير ينقص مع الوقت الي ان يصل الي الصفر ومن ثم يعطي إشارة التفجير الي القنبلة ، وكذلك الفيروس لايقوم بتنفيذ مهمتة الاساسية بمجرد تشغيلة فقد لاتتوفر الظروف او المتطلبات لذلك ، فيمكننا القول بان المفجر هو السبب الذي يدفع الفيروس الي تنفيذ الاوامر الموجوده في المدمر، قد يكون المفجر تاريخ معين او ساعه معينة فعلي سبيل المثال فيروس تشرنوبل الشهير يبقي في الحاسب الالي غير نشط الي ان ياتي يوم الاحتفال بذكري تشرنوبل وفي هذا اليوم اذا تم تشغيل جهاز الحاسب فان الفيروس يقوم بتدمير ومسح جميع البيانات الموجودة علي الحاسب الالي، وبعض الفيروس يكون المفجر الخاص بها هو انتظار المستخدم ان يضغط علي زر معين في لوحة المفاتيح او ان يضغط عدد معين من الضغطات علي زري الفارة او ان يقوم بتشغيل برنامج معين بعدها يقوم الفيروس بتنفيذ المهمة الخاصة بة فعلي سبيل المثال انت قمت ببرمجة فيروس وظيفتة منع المستخدم من تشغيل برنامج الياهو مثلا كهدف اساسي للفيروس حينها سيبقي الفيروس في الذاكرة منتظرا برنامج الياهو الي ان يعمل ومن ثم ينشط ليقوم بمنعه ثم يعود لحالة الانتظار مرة اخري، ارجو ان تكون الفكرة قد اتضحت.

الجزء الثالث: المدمر:-
وهو جزء اساسي ايضا كما وضحنا سابقا حيث يعتبر هو اشبة بالبارود الموجود في القنبلة او الديناميت اي هذا الجزء هو مايقوم بعملية التدمير وتتضح الفكرة بانة لافائدة للمفجر ان لم يتلقي جزء التدمير الاشارة منة ، فهذا الجزء هو الهدف من الفيروس او الجزء الذي سيقوم الفيروس بتنفيذة اذا ما وجد من المفجر إشارة ارسلت الية، وقد يكون المدمر اي اوامر ممكنة مثل حذف ملفات معينة كما اوضحت مسبقا او الغاء برنامج معين او ايقاف الحاسب عن التشغيل او بمعني اخر الاوامر المطلوب من الفيروس تنفيذها.

وفي الموضوعات المقبلة سوف نتعرف علي هذة الاجزاء بشكل مفصل وكيفية برمجتها وكيف تركبيها مع بعضها من اجل بناء فيروس قوي ومنظم .

الادوات اللازمة لبرمجة الفيروسات:-
لبرمجة الفيروسات فانت بحاجة الي مجموعه من الادوات اللازمة للوصول الي هذا الهدف سنستعرض اهم الادوات الازمة لعمل ذلك.
ومن هذه المتطلبات:-
١. المعرفة الجيدة بنظام التشغيل .
٢. المعرفة الجيدة بلغة برمجة معينة.
٣. مترجم خاص بلغة البرمجة.
٤. برنامج لتشفير وحماية الفيروس.

المعرفة الجيدة بنظام التشغيل:-
تعتبر هذة النقطة من اهم النقاط في طريقك نحو برمجة فيروسات قوية فنظام التشغيل هو المسؤل عن تنفيذ الاوامر الخاصة بهذا الفيروس فبدون المعرفة الجيدة بهذا النظام لن تتمكن من كتابة الفيروس بشكل سليم فعلي سبيل المثال يجب ان تفهم كيف يتعامل النظام مع العمليات وكيف يتم تشغيل البرامج وكيف يقوم النظام بالتعامل مع المكونات الصلبة للحاسب ، كل هذا حتي تكون علي دراية كافية بهذا النظام حتي لاتصاب بالهذيان اثناء برمجتك للفيروس وحتي لاتصدر كلاما خاطئا فيما يتعلق بالفيروسات حتي لاتفكر في افكار خاطئة كما قلت مسبقا علي سبيل المثال ان تطلب عمل فورمات للدرايف :C ومع العلم ان هذا القرص يحتوي علي النظام فكيف سيحدث هذا ، ويجب ايضا ان تعلم ماهي خدمات النظام System Services وكيف يتعامل النظام معها ، بالمختصر يجب ان تعلم كل كبير وصغيرة عن نظام التشغيل كل معلومة سواء كانت مهمة او غير ذلك يجب عليك ان تعلمها ان لم تستخدمها اليوم فستسخدمها غدا .

المعرفة الجيدة بلغة برمجة معينة:-
انت الان لديك العلم والفكرة لكي تكتب فيروسا فكيف لك ذلك من دون لغة البرمجة إن لغة البرمجة هي الشئ الاساسي الذي ستقوم انت من خلالة بتحقيق وبتطبيق فكرتك وتحويلها الي واقع ملموس يمكن مشاهدتة وتجربتة، ومن المعروف ان الحاسب الالي يحتوي علي العديد من لغات البرمجة الشهيرة فسنأخد علي سبيل المثال بعض هذة اللغات( BASIC- C –C++ - C#- Delphi-JAVA) الي اخر اللغات وسنقوم نحن باختيار احدي هذه

اللغات ونتعلم كل اساسيات هذه اللغة وكيف تتعامل مع الملفات والعمليات وكيف الكتابة والقراءة من الذاكرة ... الخ.
وفي شرحنا هنا سنستخد لغة البيسك وهي لغة جيدة بالنسبة للمبتدئين في هذا المجال وفيما بعد سنتكلم عن باقي اللغات الموجودة.

مترجم خاص بلغة البرمجة:-
عزيزي القارئ مافائدة لغة البرمجة بدون المترجم الخاص بها والذي وظيفتة هو تحويل الكود الذي قمت انت بكتابتة الي برنامج تنفيذي حتي يتسني لك مشاهدة التاثير عمليا وحتي تتمكن من الحصول علي ملف مستقل للفيروس، وكما قلت فاننا سوف نستخدم لغة البيسك فإننا سوف نستخدم المترجم او بيئة التطوير المتكاملة الشهيرة بالفيجوال بيسك وهذا برنامج شهير تنتجة شركة ميكروسوفت العالمية وسنستخدم الاصدار السادس.

برنامج لتشفير وحماية الفيروس:-
عزيزي القارئ لاتظن انة بترجمة الكود وحصولك علي الملف التنفيذي ستكون قد انتهيت من برمجة الفيروس، لا والف لا مازال الفيروس الخاص بك به عيبان وهما كبر الحجم نظرا لكثر الاوامر الموجودة فية والعيب الثاني هو انة يمكن بسهولة تفكيكة وإعاده قراءة الكود الخاص بة ومن ثم كشف عمليات هذا الفيروس Disassembling، ولكي نقوم بحماية الفيروس من التعديل واخفاء الكود الخاص بة سنستخدم برامج لضغط الملفات التنفيذية تسمي Packers وهذة البرامج لها القدرة علي ضغط وتشفير الكود التنفيذي للملفات التنفيذية ، وسنستخدم في شرحنا برنامج شهير يسمي UPX وهو من البرامج الرائدة في تشفير وضغط الملفات.

لماذا الفيجوال بيسك ٦؟ :-
قد يتسأل البعض لماذا تستخدم لغة الفيجوال بيسك ٦ في برمجة الفيروسات حيث هذه الإصدار قديم جدا مقارنة بالاصدارات الحديثة من هذه اللغة الرائعه لماذا مثلا لاتستخدم الدوت نيت حيث تتميز بالسهولة العالية مع استخدام كود قصير جدا مقارنة بالكود الذي ستستخدمة لكتابة الاوامر في الفيجوال بيسك ٦؟

هذا السؤال قد يطرأ علي عقول الكثير من القراء ولكن الاجابة علي هذا السؤال بسيط جدا حيث يكمن السر في استخدام هذه اللغة في انها قديمة لذلك فهي مدعومه من جميع اصدارات الويندوز التي اتت بعدها لان اي اصدار جديد من انظمة التشغيل يدعم كل اصدارات لغات البرمجة التي سبقتة وثانيا هذه اللغة لاتحتاج الي اي إضافات علي جهاز الحاسب الالي لكي تعمل فهي تعمل مستقلة وهذه الميزة يجب ان تتوفر في الفيروس الذي نقوم ببرمجتة انة يجب ان يكون مستقلا بذاتة ونقطة اخري لهذا الاصدار انة يدعم جميع اوامر النظام فلا يوجد عملية لايمكننا القيام بها بل ان كل العمليات التي نريدها نستطيع بهذة اللغة وببعض الكود ان نقوم بها ، سأوضح لك الامر جرب مثلا ان تقوم ببرمجة برنامج بلغة الفيجوال بيسك دوت نت ٢٠٠٥ وجرب ان تقوم بتشغيلة علي جهازك ماذا سيحدث؟ سيعمل البرنامح بكل بساطة وذلك لتوفر برنامج Microsoft .NET Framework 2.0 علي جهازك الشخصي ولكن جرب ان تاخد هذا البرنامج الي جهاز ليس فية برنامج الدوت نت فرام ورك ٢ فإنك ستجد صدمة وهي ان البرنامج لايعمل مظها رسالة خطا مدمر تفيد بان البرنامج لايمكنة تحديد عنوان نقطة الدخول في الذاكرة ومن ثم فان البرنامج لن يعمل ، هل تخيلت يوما ان فيروسا يطلب منك برنامجا اضافيا لكي يعمل ؟ طبعا لا فهذه ميزة اساسية في الفيجوال بيسك الاصدار السادس.

الخطوات الاولي في عالم برمجة الفيروسات:-

لن اقوم عزيزي القارئ بوضع كود بين يديك اقول لك ان هذا اول كود للفيروسات ووظيفتة عمل كذا وكذا بل حتي لن ابدا في الكلام عن برمجة الفيروسات حتي اضع بين يديك كل معلومة كبيرة كانت او صغير من الممكن ان نحتاجها في طريقنا نحو احتراف برمجة الفيروسات لانني بكل بساطة لااريدك ان تحفظ كود او شفرة دون ان تدري ما عملها او غير ذلك ساوضح لكل الامر ومن الممكن ان تفكر في طريقة اخري لانجاز هذا الامر ومن ثم تشاركنا بها فهدفنا الاول هو التعلم.

قبل ان تبدا في كتابة الفيروسات يجب ان تتعرف اولا علي كيفية عمل برنامج مضاد الفيروسات حتي تتعرف علي العدو الاول لك ولفيروسك.

يظن الكثير من المستخدمين ان برنامج مكافح الفيروسات او مضاد الفيروسات هذا برنامج خارق قام بصنعه مجموعه من الشخصيات الخارقة كأمثال سوبر مان او بات مان من اجل مكافحة البرامج الخارجة عن القانون في عالم الحاسب الالي، اقول لك عزيزي القارئ لا فبرنامج اللانتي فيروس برنامج عادي جدا بل هو برنامج تحت العادي ولكن كل مافي الامر انة يقوم بمتابعة البيانات الموجودة علي الحاسب الالي طوال الوقت ، ويمكن تدميرة وإيقافة بسهولة وسنشرح فيما بعد كيفية جعل فيروسنا يقوم بتدميرة وإيقافة عن العمل ومنعه كذلك من العمل مجددا.

ولكن دعنا الان نتعرف علي مكونات برنامج الحماية ، عادةً مايتكون برنامج الحماية من هذة الاجزاء :-

١. رادار.
٢. قاعدة بيانات الفيروسات.
٣. ميكانيكية لحجز التهديدات.
٤. ميكانيكية الفحص.
٥. لوحة تحكم.

اجل عزيزي القارئ فأي انتي فيروس في الدنيا يتكون من معظم هذه الاجزاء وقد تزيد بعض البرامج اجزاء اخري ولكن هذه الاجزاء هي الاجزاء الاساسية، وسنقوم بتوضيح كل جزء علي حدي.

الرادار:-
لاتتعجب عزيزي القارئ فانا استعمل الفاظا اقرب الي التوضيح في الواقع، الرادار كما نعلم يتم استخدامة لكي يقوم بكشف مساحة كبير من المكان قد يصل نطاقها الي مئات الكيلو مترات يعجز البشر عن كشفها في وقت قصير ، كذلك الحال في برنامج الانتي فيروس فانة فية تقنية مبرمجة داخلياً تشبه في عملها الرادار الالكتروني حيث تقوم بمتابعه كافة الملفات الموجودة علي القرص الصلب وكذلك العمليات الموجودة في الذاكرة من اجل كشف العمليات الخبيثة او التهديدات، وهو في كل هذا الوقت يستخدم ميكانيكية الفحص للتعرف علي التهديدات والفيروسات.

قاعدة بيانات الفيروسات:-
انظر معي عزيزي القارئ الي حياتنا اليومية كيف يقوم ضابط الشرطة بالتعرف علي المواطنين ، إنة يقوم بإستخدام بطاقة تحديد الهوية ومن ثم يبحث عن الشخص في جهاز الحاسب الالي لعرض بياناتة، كذلك الحال في برنامج الانتي فيروس فهو يتعرف علي الفيروسات باستخدام قاعده بيانات مخزن فيها اسم الفيروس وتوقيعه ، ولكن ماهو التوقيع ؟ التوقيع عبارة عن قيمة مسجلة بالهكس للفيروس وهي قيمة مميزة في شفرة الفيروس تمكن المكافح من التعرف علية بهذة العلامة .

ميكانيكية الفحص:-
كما قلت من قبل ان ميكانيكية الفحص هي تشبه في عملها عمل ضابط الشرطة الذي يتعرف علي المواطنين ببطاقة الهوية ، كذلك الحال ايضا في برنامج الانتي فيروس فان ميكانيكة الفحص تقوم باستدعاء الملف ومن ثم تقوم بالبحث في بنيتة عن اي توقيع مشابة للتوقيعات الموجوده في قاعده البيانات وان وجد التوقيع فإنها تسلم الملف الي ميكانيكية الحجز لكي تقوم بعمل الاجراءات اللازمة لوقف هذا التهديد، أما اذا لم يجد تهديد فإنة ينتقل الي الملف التالي بكل بساطة، وتستخدم ميكانيكية الفحص بشكا مستمر قاعده البيانات الفيروسية.

ميكانيكية حجز وإيقاف التهديدات:-
تلعب ميكانيكية الحجز وإيقاف التهديدات دورا مهما في الانتي فيروس فهي تلعب دور القبض علي المجرم في عالمنا ، وكما هو الحال في المكافح فبدون هذه الميكانيكية لن يتمكن المكافح من

الامساك بالتهديدات ، نعم هو سيتعرف علي التهديدات ولكنة لن يتمكن من الامساك بها ومن ثم إيقافها، تمتلك ميكانيكة الحجز خوارزمية خاصة لتشفير ملفات التهديدات التي يتم الامساك بها من اجل منع المستخدم من تشغيلها نظرا لاحتوائها علي تهديد وكذلك يملك اساليب الحذف بالقوة المعروفة ويملك ايضا الوسائل اللازمة لايقاف العمليات من الذاكرة.

لوحة التحكم:-
عزيزي المستخدم ان برنامج الانتي فيروس بدون لوحة التحكم كالصاروح الذي لايستطيع احد ايقافة او التحكم بة ، فبلوحة التحكم يمكنك تحديد مستوي الحماية ومن خلالها ايضا يمكنك إيقاف وتشغيل دروع الحماية ، فبإختصار شديد هي حلقة الوصل بين البرنامج والمستخدم.

كان هذا بإختصار شديد المكونات الاكثر شهر لبرنامج الانتي فيروس.
أما اذا تحدثنا عن انواع برنامج الانتي فيروس فهما بإختصار شديد نوعان:-

١. Static Antivirus
٢. Dynamic Antivirus

وسنشرحهم بالتفصل في الجزئية القادمة.

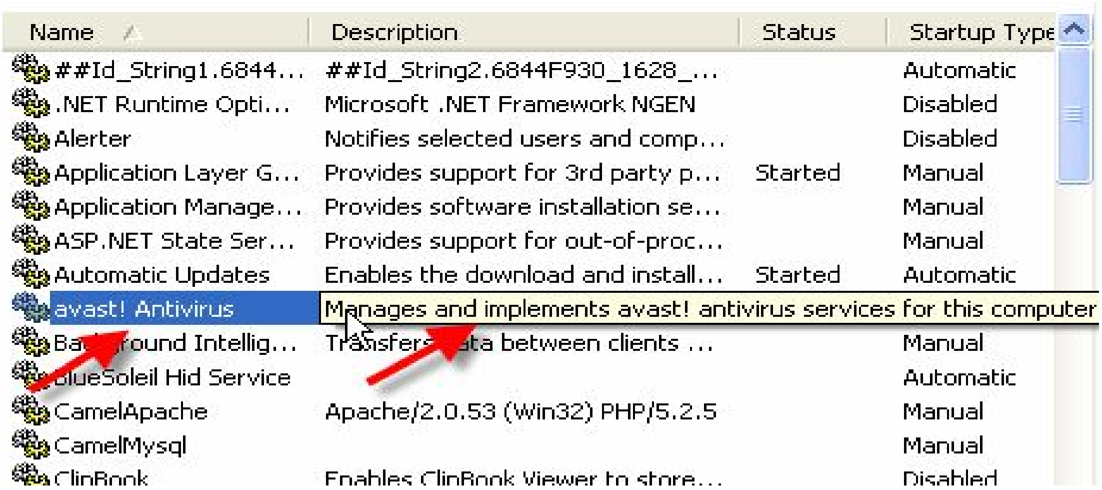
النوع الاول : مضاد الفيروسات الثابت Static antivirus :-
يكمن الاختلاف في نوعي برنامج مضاد الفيروسات الي ميكانيكية الفحص المستخدمة لأكثر، فهذا النوع من البرامج ويسمي بالانتي فيروس الثابت او العادي يتميز بان لدية قاعده بيانات تحتوي علي كل تواقيع الفيروسات وتتم إضافة التواقيع في القاعده بواسطة الشركة المصنعه لهذا المكافح ومن ثم يقوم المستخدم بتحديث قاعده بيانات برنامجة لكي يتعرف علي احدث التهديدات ولكن مايعيب هذا المكافح هو عدم قدرتة علي التعرف علي التهديدات الغير موجودة في قاعده بياناتة وعيب اخر فية هو نظرا لكثرة عدد الفيروسات الموجوده في عالم الحاسب الالي فإنة ببساطة شديدة يملك قاعده بيانات كبيرة الحجم تستغرق وقتا في تحديثها ولكن ميزة هذا المكافح انة يمكنة التعرف علي الفيروسات في اي نوع من الملفات وفي اي نظام تشغيل مختلف .وهذا النوع يحتاج الي التحديث المستمر لقاعدة

البيانات للتعرف علي احدث التهديدات.وهذا النوع من المكافحات لايمكن ان يصدر اليك رسالة تهديد بفيروس مزيفة بمعني انة اذا اظهر رسالة تهديد فتاكد حتما بان هذا الملف بة فيروس.

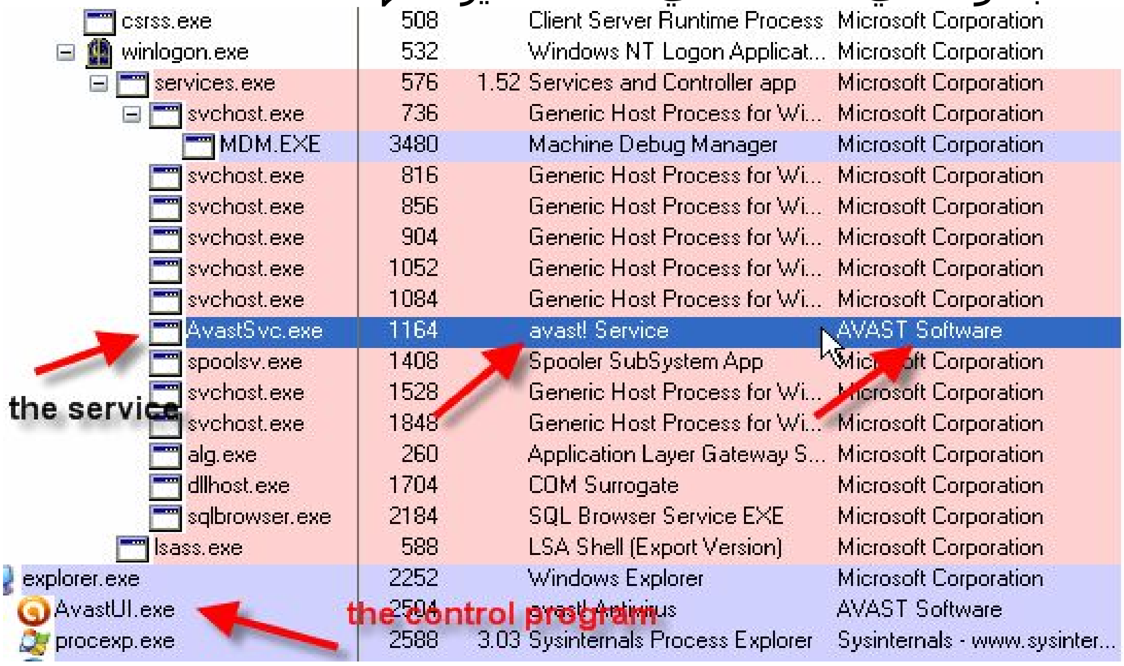
النوع الثاني: مضاد الفيروسات المتغير Dynamic antivirus :-
يتميز هذا النوع من مضادات الفيروسات بانة مبرمج علي التعرف علي طرق التهديدات وكيفية التعرف علي التهديدات من اي برنامج مهما كان سواء كان موجود في القاعدة او لا لذلك يمكن الاعتماد علي هذا المكافح في التعرف علي التهديدات المختلفة ولكن يعيب هذا النوع من المكافحات هو انة من الممكن ان يتعرف علي برنامج ليس خبيث علي انة برنامج خبيث اذا وجد منة تشابة في بعض الصفات مع التقنيات المخزنة لدية والتي يفحص وجودها في الملفات ، وأيضا من عيوب هذا النوع هو انة لايمكنة ان يتعرف علي الفيروسات خارج نظام تشغيل معين فهو صمم من اجل نظام تشغيل واحد فقط وهو لايحتاج تحديث مستمر لقاعده البيانات بل يجب تنزيل احدث الاصدارات منة دائما.

بنية برنامج مضاد الفيروسات:-
يتم بناء برنامج الانتي فيروس كجزئين اساسيين هما:
١. برنامج الخدمة.
٢. برنامج التحكم.

برنامج الخدمة:-
الخدمة هي عبارة عن برنامج يعمل في بيئة التشغيل ويندوز صمم بطريقة خاصة لكي يعمل بطريقة خاصة لتادية مهام معينة تحت اشراف نظام التشغيل ، وهذه الخدمة تحتوي علي ميكانيكية الفحص ، الرادار ، وميكانيكية ايقاف التهديدات.وهي برنامج لايمكنك ايقافة من اي مدير للمهام.
ويمكنك الوصول الي الخدمات الموجودة في النظام عن طريق كتابة services.msc في مربع التشغيل Run ومن ثم قم بالبحث عن الخدمة التي تحتوي علي اسم مكافح الفيروسات خاصتك في قائمة تظهر لك كما بالشكل:



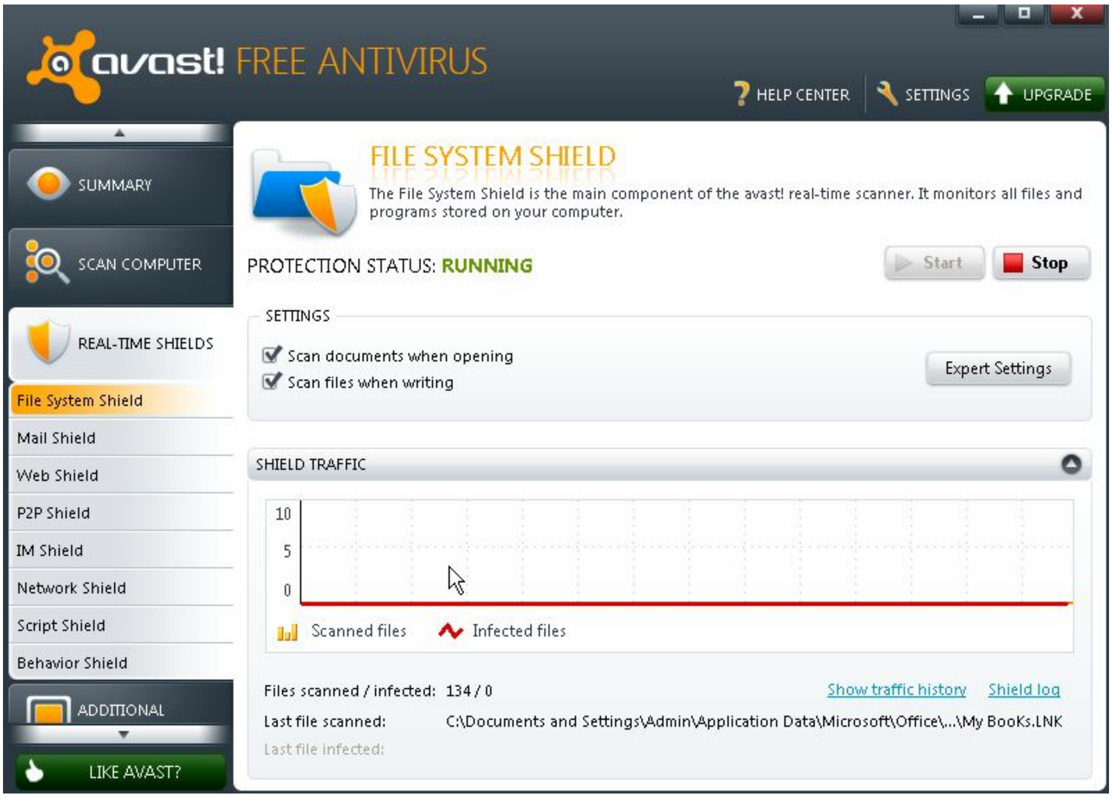

حيث انني اتعامل مع برنامج Avast Antivirus وهذه هي الخدمة الخاصة بة وهاهي الخدمة في قائمة مدير المهمات:



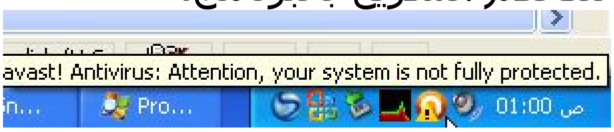

حاول ان تغلقها ،لن تستطيع فهي محمية وسنتعلم فيما بعد كيف نمكن الفيروس الخاص بنا من تدمير هذه العملية.

برنامج التحكم:-

كما قلنا سابقا فإن برنامج التحكم هو حلقة الوصل بين المستخدم وبرنامج الحماية وهي برنامج عادي يمكنك من خلالة التحكم ببرنامج المكافح الخاص بك وضبط مسنوي الحماية او تحديث قاعدة البيانات، وشكل لوحة التحكم الخاص ببرنامج الانتي فيروس الخاص بي كالتالي:




وهذا البرنامج لة ايقونة بجوار ساعه النظام  كما بالشكل للوصل للتحكم السريع بالبرنامج:




وهذه العملية هي عملية عادية يمكن ايقافها من اي مدير للمهمات.

كل هذه المعلومات الاساسية يجب ان تعلمها عن مكافح الفيروسات حتي تتمكن من العمل في هذا الطريق بسلام.

بهذا الجزء نكون قد انتهينا من الاساسيات وندخل في الشرح بدأً من الموضوع القادم .

لاتنسي زيارة مدونة الامن والحماية والفيروسات
http://xredcodex.blogspot.com/